

Appl. No.: 09/774,999

APP 1357

Amdt. Dated: August 10, 2004

Reply to Office Action of: April 29, 2004

Amendments to the Specification:

Please replace the paragraph beginning at page 1, line 6, with the following rewritten paragraph:

This application is related to commonly owned U.S. patent application serial no. ~~(Attorney Docket APP-1300)~~ 09/774,964 filed concurrently herewith and entitled "System and Method For Out-Sourcing The Functionality of Session Initiation Protocol (SIP) User Agents to Proxies." This application is also related to commonly owned U.S. patent application serial no. ~~(Attorney Docket APP-1257)~~ 09/775,000 filed concurrently herewith and entitled "Smart Appliance Network System and Communication Protocol."

Please replace the paragraph beginning at page 2, line 1, with the following rewritten paragraph:

Networked Appliances (NAs) are dedicated consumer devices containing at least one networked processor. As an alternative, conventional appliances can be connected to an appliance controller which accepts remote messages and controls the appliance in the desired way. As a result, a substantial amount of computing power is ~~need~~ needed in each controller.

Please replace the paragraph beginning at page 3, line 1, with the following rewritten paragraph:

The Internet Engineering Task Force ("IETF") has developed a communications protocol called Session Initiation Protocol ("SIP") which can accommodate a number of different modes of communication. SIP, according to proposed standard RFC 2543, is an application-layer control and signaling protocol for creating, modifying and terminating interactive communications sessions between one or more participants. It is a text-based protocol similar to HTTP and SMTP. These sessions may include voice, video, chat, interactive games and virtual reality, e.g., Internet multimedia conferences, Internet telephone calls and multimedia distribution. Members in a session can communicate via multicast or via a mesh of unicast relations, or a combination of these.

Please replace the paragraph beginning at page 9, line 4, with the following rewritten paragraph:

According to the present invention SIP is to be used as the basic architecture to implement remote appliance control. However, before it can be used for this purpose, certain changes must be made. In particular, in SIP, the names that are found in the "To:" and "From:" fields are encoded as Universal Resource Locators (URL). Current implementations support SIP and PHONE URLs. However, a new type of URL must be defined for Networked Appliance systems without changing the nature of the protocol. This new URL type allows for "user friendly" discovery of the appliance address. An ~~example~~, example using the service URL syntax defined in RFC2609, ~~but~~, but without the location information (which has already been determined via the SIP routing) and without the "sip:" prefix would be:

Please replace the paragraph beginning at page 12, line 8, with the following rewritten paragraph:

The SIP Instant Messaging system defines two new primitives, SUBSCRIBE and ~~NOTIFY~~ NOTIFY, that can be used to achieve asynchronous communications. When these

Appl. No.: 09/774,999
Amdt. Dated: August 10, 2004
Reply to Office Action of: April 29, 2004

APP 1357

two methods are used in conjunction with the proposed addressing scheme and the Device Messaging Protocol MIME type, then event notification from and between Networked Appliances is enabled.

Please replace the paragraph beginning at page 12, line 13, with the following rewritten paragraph:

Fig. 1 shows a typical prior art SIP architecture. In this arrangement, a client, e.g., an Internet phone user, employs a SIP User Agent application operating as a client, i.e., SIP UAC 100, to initiate a SIP communication with one or more User Agent Servers (UAS) ~~which that~~ may be associated with an intended recipient of an Internet phone call. This system supports three different types of architectures which permit remote communication with networked devices. The actual implementations may use any combination of the three architectures.

Please replace the paragraph beginning at page 12, line 20, with the following rewritten paragraph:

In the first arrangement, the client application UAC 100 is able to directly connect to and interact with one of several UAS devices 110, 112, 114, 116 and 118. In this case the client establishes contact directly with the UAS 110 at the recipient via path 130. The second architecture has the client application interact with a SIP proxy 104 in the Internet in order to communicate with networked devices, e.g., Internet phones. In the second architecture, ~~another~~ SIP proxy 104 passes communications from UAC 100 to one of the various SIP UAS devices, e.g. UAS 110, via path 132.

Please replace the paragraph beginning at page 15, line 26, with the following rewritten paragraph:

In the arrangement of Figs. 2-3, the SIP UAS as shown in Fig. 1 has been considered to be the residential gateway (RGW). However, in an alternative embodiment, the Internet capable appliance 202 and the appliance controller 204 may be considered SIP UAS devices, with the RGW as their proxy server. However, in ~~the this~~ arrangement the UAS device would not need address mapping capability, unless for example the controller 204 controlled more than one appliance.

Please replace the paragraph beginning at page 17, line 8, with the following rewritten paragraph:

The Interworking Unit ~~206 208~~ maps the appliance message carried in the payload of the SIP message into the appliance-specific protocol. This protocol is in a form that can be interpreted by the non-IP appliances 206 which are thus controlled by the appliance controller 204 through the use of the Interworking Unit 208 in order to communicate/interact with the originating client applications.

Please replace the paragraph beginning at page 17, line 13, with the following rewritten paragraph:

The SIP UAS (IP capable appliance) 202 resides in an IP (SIP) capable Networked Appliance. It terminates SIP appliance control messages from the originating application SIP UAC 100, and retrieves the appliance control status information for the appliance application, acting on it directly without any requirement for an intervening Interworking Unit ~~206 208~~ or a appliance controller 204 which are needed for the non-IP appliance.

Appl. No.: 09/774,999
Amdt. Dated: August 10, 2004
Reply to Office Action of: April 29, 2004

APP 1357

Please replace the paragraph beginning at page 17, line 19, with the following rewritten paragraph:

The key interfaces in Fig. 5 are (1) the SIP Networked Appliances, (2) the appliance registration and location, and (3) the appliance specific interfaces. The SIP appliances interface represents IETF SIP with the DO method for communicating with Networked Appliances. The appliance registration and location interface is achieved with any appropriate database update and lookup protocol which is used to access the location database 140. Examples of such a protocols are LDAP and SLP. Further, the appliance-specific interfaces are numerous home-networking technologies currently available. It is the function of the Interworking Unit ~~206~~ 208 to map from SIP to the protocols of the specific technology of the target appliance.

Please replace the paragraph beginning at page 21, line 1, with the following rewritten paragraph:

The above scenario could also be used to depict a failure scenario. Once the lamp receives the message, it may realize that its bulb is "blown" (broken) and in response ~~sends~~ sends something like:

Please replace line 22 at page 22 with the following rewritten line:

4. DO sip:[d=lamp,r=~~bedroom~~ spareroom,u=stanm]@ua.simon.home.net
SIP/2.0

Please replace line 11 at page 32 with the following rewritten line:

~~3~~ 3. OPTIONS sip:[d=vcr,r=den]@dilbert.home.net SIP/2.0

Please replace line 18 at page 32 with the following rewritten line:

~~2~~ 4. SIP/2.0 200 OK

Please replace line 1 at page 33 with the following rewritten line:

~~2~~ 5. SIP/2.0 200 OK

Please replace line 12 at page 33 with the following rewritten line:

~~3~~ 6. SIP/2.0 200 OK

Please replace line 6 at page 34 with the following rewritten line:

+ 2. Proxy forks the following messages:

Please insert a blank line between lines 11 and 12 at page 34.

Please replace lines 23 and 24 at page 34 with the following rewritten lines:

*Printer B responds with OK
* ~~3~~ 3. SIP/2.0 200 OK

Please replace line 4 at page 35 with the following rewritten line:

Page 4 of 15

Appl. No.: 09/774,999
Amdt. Dated: August 10, 2004
Reply to Office Action of: April 29, 2004

APP 1357

w 4 SIP/2.0 200 OK

Please replace the paragraph beginning at page 37, line 14, with the following rewritten paragraph:

In general, a user will not want a passive eavesdropper to be able to determine the content of a message. This applies not only to the body of the message (which will contain the command to be executed), but also to header fields which may leak information about the devices one owns. For example, the "To:" header field will contain a URL of the addressed ~~entity which~~, entity, which will indicate the device type and location. A user may not want anyone to know whether he owns a television, and he certainly would not want anyone to know the room in which the television is located.

Please replace the paragraph beginning at page 39, line 7, with the following rewritten paragraph:

For general SIP security, some form of public-key technology must be employed to provide security according to the Handley et al. proposal. In the case of remote access to NAs within the ~~home~~, home, however, shared secrets can be used to provide privacy and authentication. There are two primary reasons for this difference: first, general SIP communication can potentially occur between any two parties, while in the case of remote access to the home a one-to-one (or few-to-one) correspondence exists between authorized users and the homes to which they will be communicating. Second, general SIP communication frequently occurs between parties who have had no prior contact, and therefore no opportunity to generate a shared secret. In the case of home access, however, users will have the opportunity to designate a shared secret for use in their communication with the home. The secret may be shared either with the home RGW/firewall (in the case of direct communication from user to the home, as in Figure 1) or with the Service Provider Proxy (in the case of Communication via Proxy, as in Figure 4).